AMENDMENTS TO THE CLAIMS

Following is a listing of all claims in the present application, which listing supersedes all

previously presented claims:

Listing of Claims:

1.   (Currently Amended) A cryptographic method using dual keys in a wireless local

area network (LAN) system, comprising:

(a) generating a first group key in N wireless terminals forming an ad-hoc group, where

N is equal to or greater than two;

(b) generating a second group key in a main wireless terminal to perform a key

distribution center function among the N wireless terminals, and transmitting the second group

key to (N-1) sub wireless terminals; [[and]]

(c) encoding data using the second group key, and transmitting the encoded data between

the N wireless terminals, and

(d) modifying the second group key in the main wireless terminal according to a

modification time period, predetermined in the main wireless terminal, and transmitting the

modified second group key to the (N-1) sub wireless terminals.

2.   (Original)   The method as claimed in claim 1, wherein the first group key is

generated using a group password of the ad-hoc group.

3.   (Original)   The method as claimed in claim 1, wherein in (b), the main

wireless terminal encodes the second group key using the first group key, and transmits the

encoded second group key to the (N-1) wireless terminals.

4.   (Original)   The method as claimed in claim 1, wherein the main wireless

terminal is a creator of the ad-hoc group.

5.   (Currently Amended) The method as claimed in claim 1, wherein when the main

wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a

~~function of~~ key distribution center function to a sub wireless terminal selected from among the

(N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal.

6.   (Canceled).

7.   (Currently Amended) The method as claimed in claim [[6]] 1, wherein in (d), the

modified second group key is encoded using a non-modified second group key, and transmitting

the encoded second group key to the (N-1) sub wireless terminals.

8.   (Original)   The method as claimed in claim 1, wherein (b) comprises:

(b1) if the first group key is created, encoding a second group key request message from

one of the (N-1) sub wireless terminals, and transmitting the encoded second group key request

message to the main wireless terminal;

(b2) decoding the second group key request message, using the first group key, in the

main wireless terminal; and

(b3) creating a second group key according to the decoded second group key request

message, in the main wireless terminal.

9.   (Currently Amended) A tangible computer readable medium having embodied

thereon a computer program for the method according to claim 1.

10.   (Currently Amended) A <u>tangible</u> computer readable medium having embodied

thereon a computer program for the method according to claim 3.

11.   (Currently Amended) A <u>tangible</u> computer readable medium having embodied

thereon a computer program for the method according to claim 8.

12.   (Currently Amended) A wireless local area network (LAN) system, comprising:

N, where N is equal to or greater than two, wireless terminals which form an ad-hoc

group, and create [[a]] first <u>and second</u> group [[key]] <u>keys</u>, wherein the N wireless terminals

include:

a main wireless terminal for performing a key distribution center function in the ad-hoc

group, for creating a second group key and encoding data using the second group key, and for

transmitting the encoded data between the remaining wireless terminals; [[and]]

(N-1) sub wireless terminals for <u>generating a first group key and for</u> receiving the second

group key from the main wireless terminal and encoding data using the second group key, and

for transmitting the encoded data between the remaining wireless terminals<u>, and</u>

wherein the second key management unit modifies the second group key according to a

modification time period, predetermined in the main wireless terminal, and transmits the

modified second group key to each of the (N-1) sub wireless terminals.

13.   (Original)   The system as claimed in claim 12, wherein the first group key is

generated using a group password of the ad-hoc group.

14.   (Original)   The system as claimed in claim 12, wherein the main wireless

terminal encodes the second group key using the first group key, and transmits the encoded

second group key to the (N-1) wireless terminals.

15.   (Original)   The system as claimed in claim 12, wherein the main wireless

terminal is a creator of the ad-hoc group.

16.   (Currently Amended) The system as claimed in claim 12, wherein when the main

wireless terminal is withdrawn from the ad-hoc group, the main wireless terminal transfers a

~~function of~~ key distribution center <u>function</u> to a sub wireless terminal selected from among the

(N-1) sub wireless terminals, so that the sub wireless terminal acts as the main wireless terminal.

17.   (Currently Amended) The system as claimed in claim 12, wherein [[the]] <u>each</u>

sub wireless terminal comprises:

a first group key generator for creating a first group key using a group password input

from a user;

a first encryption unit for storing the first group key, for encoding a second group key

request message, using the first group key, for decoding a second group key response message

from the main wireless terminal using the first group key, and for encoding data input from a

user using a second group key; and

a first key management unit for generating the second group key request message to

output to the first encryption unit, for extracting a second group key from the second group key

response message decoded in the first encryption unit, and for outputting the extracted second

group key to the first encryption unit.

18.   (Original)   The system as claimed in claim 12, wherein the main wireless

terminal comprises:

a second group key generator for creating a first group key using a group password input

from a user;

a second encryption unit for storing the first group key, for decoding the second group

key request message transmitted from the sub wireless terminal using the first group key, for

encoding the second group key response message for transmitting to the sub wireless terminal

using the first group key, and for encoding data input from a user using the second group key;

and

a second key management unit for receiving the second group key request message

decoded from the second encryption unit, for creating the second group key, and for outputting

the second group key response message including the created second group key to the second

encryption unit.

19.   (Canceled).

20.   (Currently Amended) The system as claimed in claim [[19]] 12, wherein the

second encryption unit encodes the modified second group key using a non-modified second

group key, and transmits the encoded modified second group key to each of the (N-1) sub

wireless terminals.

21.   (New) A wireless terminal using dual keys for cryptography, the wireless

terminal comprising:

a group key generator for creating a first group key using a group password input from a

user;

an encryption unit for storing the first group key, for encoding a group key response

message corresponding to a group key request message transmitted from at least one wireless

terminal, by using the first group key, for transmitting the encoded group key response message

to the at least one wireless terminal, and for encoding data input from a user using a second

group key; and

a key management unit for receiving the group key request message, for creating the

second group key, for outputting the group key response message including the created second

group key to the encryption unit, and for modifying the second group key according to a

predetermined modification time period.

22.   (New) The wireless terminal as claimed in claim 21, wherein the encryption unit

encodes the modified second group key using a non-modified second group key, and transmits

the encoded modified second group key to the at least one wireless terminal via the encryption

unit.

23.   (New) A wireless terminal using dual keys for cryptography, the wireless

terminal comprising:

a group key generator for creating a first group key using a group password input from a

user;

an encryption unit for storing the first group key, for encoding a group key request

message, by using the first group key, for decoding a group key response message, by using the

first group key, and for encoding data input from a user using a second group key which is

modified according to a predetermined modification time period; and

a key management unit for generating the group key request message to output to the

encryption unit, for extracting the second group key from the decoded group key response

message, and for outputting the extracted second group key to the encryption unit.